

Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)

Approved for use through xx/xx/200x. OMB 0651-00xx

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW		Docket Number (Optional) 299002053200	
	Application Number 09/894,203	Filed June 28, 2001	
	First Named Inventor Ichiro TOMOHIRO		
	Art Unit 2136	Examiner D. G. Cervetti	
<p>Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.</p> <p>This request is being filed with a notice of appeal.</p> <p>The review is requested for the reason(s) stated on the attached sheet(s). Note: No more than five (5) pages may be provided.</p> <p>I am the</p> <p><input type="checkbox"/> applicant/inventor.</p> <p><input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96)</p> <p><input checked="" type="checkbox"/> attorney or agent of record. Registration number 54,217</p> <p><input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34</p> <p>Signature Adam Keser Typed or printed name (703) 760-7301 Telephone number April 24, 2007 Date</p> <p>NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representatives(s) are required. Submit multiple forms if more than one signature is required, see below.</p> <p><input type="checkbox"/> *Total of 1 forms are submitted.</p>			

va-202127

1

APR 24 2007

Docket No. 299002053200

(PATENT)

Clnet Reference No.: F5-01965232/01R00118-1US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Ichiro TOMOHIRO

Application No. 09/894,203

Confirmation No. 7078

Filed: June 28, 2001

Art Unit: 2136

For: SEMICONDUCTOR STORAGE DEVICE

Examiner: David G. Cervetti

PRE-APPEAL BRIEF REQUEST FOR REVIEW

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant respectfully requests review of the Action mailed February 12, 2007, for the reasons set forth below. Applicant is filing a Notice of Appeal concurrently herewith.

I. Vicard does not disclose storing both a key and a lock

Claims 1-10 stand rejected under 35 USC 102(b) on Vicard (U.S. Patent No. 5,708,715).

Vicard only discloses storing one element, regardless of which element (a key or a lock) is stored in Vicard, the other element is not stored. Vicard discloses a semiconductor memory incorporating a conventional data tamper prevention circuit similar to that depicted in applicant's Figure 3, and does not disclose or suggests "at least one memory region ... *for storing the security release key; [and] at least one non-volatile storage means for storing a security registration lock*" (emphasis added). Instead, the system of Vicard requires that a chip-key be supplied to a lock circuitry from a source external to the chip (Vicard, col. 4, lines 43-45).

I

va-202117

Application No.: 09/894,203

Docket No.: 299002053200

The Examiner has asserted that “the key stored in hashed format is the release key since it is used to determine whether the circuit is to be unlocked or not. The hash, encrypted key is stored within the chip and a received encrypted key is submitted to the same hash function to later determine if a match exists (Vicard, summary of the invention, columns 3-6). ... Vicard clearly teaches having stored a hash of a key (a key on its own right)”.

However, even if Vicard did disclose storing a key, Vicard does not disclose storing *both* a key and a lock as recited in claim 1. At best, Vicard only discloses storing a signature of a correct chip-key in the register 25 shown in Fig. 1 (see Vicard, col. 4, lines 62-66).

Vicard discloses inputting an external chip-key and decrypting the externally input chip-key at the secure communications module 20, such that a first intermediate chip-key output IV1 is sent to the one-way hash function module 26 to be hashed. The intermediate hashed chip-key IV2 is then compared to the stored signature of a correct chip-key at the comparator 27. While the Examiner asserts that the stored signature of Vicard discloses the security release key recited in claim 1, applicant respectfully submits that even if the stored signature were equivalent to the stored release key of claim 1, which it is not, Vicard would then fail to disclose or suggest storing the security registration lock in a nonvolatile storage, as recited in claim 1. Vicard only discloses storing one element, the signature. Consequently, regardless of which element (a key or a lock) is stored in Vicard, a second element is not stored.

II. The Examiner mistakenly equates comparing two keys with comparing a key to a lock

The Examiner asserts, in the Advisory Action mailed February 12, 2007, that applicant's arguments are unpersuasive because “Vicard teaches storing a signature of a correct chip-key and a decryption key, since the input is received in an encrypted form (col. 3, lines 40-50), decrypting the input to produce a first value, and applying a hash function to this value to produce a second value (col. 4, lines 43-61, and claims 1-6), Vicard further teaches using 2 or more chip-keys (col. 6, lines 20-36).”

Application No.: 09/894,203

Docket No.: 299002053200

By asserting that the hash encrypted key that is stored in the chip is the release key, and that a received encrypted key is submitted to the same hash function to later determine if a match exists, the Examiner takes the position that "a key" (the hash, encrypted key, as a release key) is compared with another "key" (received encrypted key). This interpretation is not consistent with the concept of a security "lock" and "key" configuration as disclosed and claimed by applicant, where a received "key" is compared with a stored "lock." In such configurations, when a received key matches a stored lock a security function is released. Instead, the Examiner appears to assert that a received "key" is compared with a stored "key," which is not what applicant claims

III. The Examiner has failed to address applicant's arguments that the chip-key of Vicard cannot correspond to the security release key

The Examiner has failed to address applicant's arguments that Vicard requires that the chip-key be externally supplied to the lock circuitry of the chip (see, e. g. , column 4, lines 43-45 of Vicard), i.e., *not stored in the chip*. The chip-key of Vicard cannot correspond to the security release key of this invention because, in Vicard, the chip-key is input by a user (from a source external to the chip) in contrast to the features of claim 1, where the security release key is stored in the at least one memory region, each one of said at least one memory region being provided in the at least one memory cell array block.

Vicard discloses that "[i]n order to ascertain whether an input chip-key is the correct one to unlock the particular chip 10 concerned, the lock circuitry further comprises a one-way function block 26 that subjects the chip-key output as IV1 from block 20 to the one-way function (in this case, the SHA) used to form the chip-key signature held in register 25. The resultant intermediate value hash encrypted key that is stored in the IV2 output by block 26 is then compared in comparison block 27 with the signature stored in register 25; if a match is found, the comparison block 27 outputs an enable signal on line 19 to cause operational enablement of the functional block 12." (Vicard, col. 5, lines 10-24).

Application No.: 09/894,203

Docket No.: 299002053200

In relation to claim 1, the signature of the chip-key of Vicard may correspond to the "security registration lock" that is stored in the at least one nonvolatile storage means (see applicant's Non-volatile register 13 of Figure 1 and paragraphs [0053] to [0055]).

As noted in applicant's specification, the conventional technique as shown in Figure 3 (which is noted above as being similar to the invention as disclosed by Vicard) has at least the following problems:

First, in order to release the function limitation, it is necessary to externally input a function limitation release key. Accordingly, the above-described system *requires an external key storage device* for storing the function limitation release key. However, since the function limitation release key is retained external to the device, *the key must pass through an interfacing section every time access is requested, independent of what sort of encryption technique may be employed in the communication path between the devices, i.e., between the device shown in FIG. 3 and any other device within the system (e.g., the key storage device). This may run the risk of the function limitation release key being intercepted during communication, or being directly read from the external key storage device.*

Moreover, *complicated circuitry is required for encrypting signals exchanged between devices*, and particularly complicated encryption is required. Hence, complicated decoding circuitry within the device is required to provide protection against repetitive attacks; and

Furthermore, in order to effectuate a good tamper prevention function, merely replacing a given semiconductor storage device with a semiconductor storage device having a tamper prevention function does not suffice. In addition, *the entire system must be redesigned to enable a good tamper prevention function"*.

(Emphasis added). See, paragraphs [0009] to [0011] of applicant's specification; and col. 4, lines

APR 24 2007

Application No.: 09/894,203

Docket No.: 299002053200

43-61 of Vicard, wherein Vicard discloses the encryption and decryption that are required.

Furthermore, Examiner's assertion that the hash encrypted key that is stored within the chip is the claimed security release key is inconsistent with the teachings of Vicard and with the general concept of a "lock" and "key" arrangement as discussed above. To the contrary, it is pointed out that the hash encrypted key is stored in register 26 of the lock circuitry 11 of Vicard (Vicard, Fig. 1, and col. 4, line 65 to col. 5, line 9), such that Vicard does not disclose or suggest that the "key" (i.e., the security release key) is stored in the semiconductor storage device (i.e., in at least one memory region thereof).

IV. Conclusion

In light of the above, the rejections of record are improper and should be withdrawn. A Notice of Allowance is thereby solicited.

In the event that the transmittal letter is separated from this document and the Patent and Trademark Office determines that an extension and/or other relief is required, applicants petition for any required relief including extensions of time and authorize the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to Deposit Account No. 03-1952, referencing Docket No. 299002053200.

Dated: April 24, 2007

Respectfully submitted,

By 

Adam Keser

Registration No.: 54,217

MORRISON & FOERSTER LLP

1650 Tysons Blvd, Suite 400

McLean, Virginia 22102

(703) 760-7301